September 16, 2010

VIA ELECTRONIC FILING

Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

RE: ET Docket No. 04-186 Unlicensed Operation in the TV Broadcast Bands

Ex Parte Communication

Dear Ms. Dortch:

On September 14, 2010, Jesse Caulfield from Key Bridge Global LLC, Jude Boyle and Robert Crissy from Oracle, Gene Stromecki and Paul Jefferson from Fortinet Inc. met with the following representatives from the Office of Engineering and Technology: Julius Knapp, Chief, Ira Keltz, Deputy Chief, Geraldine Matise, Chief of Policy & Rules, Walter Johnston, Chief of Electromagnetic Compatibility, Michael Ha of the Technical Analysis Branch, Hugh van Tuyl Senior Electronics Engineer, and Peter Georgiu, Electronics Engineer.

In the meeting, Key Bridge summarized the most important aspects of our petition for reconsideration and other related filings[1]. Key Bridge explained our understanding of the FCC's desired intent for allowing unlicensed white space operation, and discussed Key Bridge's conclusion that in order to successfully achieve this intent the FCC White Space rules must require authentication of database administrators and white space devices (WSDs).

We explained our interpretation of current rules as requiring device and database *identification*, which is distinct from *authentication* and does not imply or require a verifiable binding between an internet IP address and the credentials it submits (FCC ID plus Serial Number for example).

The Key Bridge team explained that, in our perspective, database authentication is a solved problem and may be implemented with server-based certificates in a practice similar to conventional secure web services.

The parties discussed the fact that the FCC has not required authentication for other wireless technologies like cellular telephony, WiFi, WiMax, etc. but that the FCC has also not allowed those frequency allocations to implement white space spectrum sharing nor compelled such systems to use an administrator for interference avoidance.

[1] See Key Bridge Global *Petition for Reconsideration* submitted 03/19/09, *Consolidated Opposition to Petitions for Reconsideration* submitted 05/08/09, *Reply to Oppositions* submitted 05/18/09, *Ex Parte* submitted 06/09/09 regarding device authorization, *Ex Parte* document submitted 08/17/09 entitled *Registration, Authentication and Security*, Joint *Ex-Parte* by Key Bridge Global LLC, WSdb LLC, Frequency Finder Inc., KB Enterprises LLC, Spectrum Bridge, Telcordia Technologies submitted 02/12/10 regarding multiple database administrators, *Comments of Key Bridge Global LLC* submitted 02/12/10.

Key Bridge noted that device authentication is necessary for administrators to successfully implement rules compliance without undermining its central purpose of interference avoidance: because administrators must provide service on a non-discriminatory basis[2], present rules require service to any device presenting valid identification (FCC ID and Serial Number) and this requirement does not anticipate forged credentials; which authentication would prevent. Additionally, an administrator's ability to support FCC enforcement action[3] is impaired and may be effectively disabled without the corresponding ability to positively identify individual devices, a capability only available through device authentication.

Key Bridge noted that large-scale mutual authentication technologies exist and are in operation today that could readily support white space devices numbering in the tens of millions. As examples, we cited the embedded hardware-based certificates in certain models of smart phones, computers, Femtocell devices and WiMax radios.

Lastly, Key Bridge stressed that device authentication via a verifiable binding between a white space device and its credentials does not require or imply end-user identification, and that the examples cited (smart phones, computers, Femtocell, WiMax) uniquely identify the device while preserving user anonymity. The Key Bridge team then reminded the Commission of our solution's comprehensive information security and user data protection strategies[4].

By request, Key Bridge suggests the following rule edits that would implement the type of authentication we believe is necessary to achieve the FCC's stated goals for successful white space implementation, adoption and operation.

Revise 15.711(b)(3)(i) to read as follows:

> (3)(i) Fixed devices must access and authenticate themselves to a TV bands database over the Internet to determine the TV channels that are available at their geographic coordinates prior to their initial service transmission at a given location. Operation is permitted only on channels that are indicated in the database as being available for TVBDs. Fixed TVBDS shall access the database at least once a day to verify that the operating channels continue to remain available. Operation must cease immediately if the channel is no longer available.

Revise 15.711(b)(3)(ii) to read as follows:

> (ii) Mode II personal/portable devices must access and authenticate themselves to a TV bands database over the Internet to determine the TV channels that are available at their geographic coordinates prior to their initial service transmission at a given location. Operation is permitted only on channels that are indicated in the database as being available for TVBDs. A Mode II personal/portable device must access the database for a list of available channels each time it is activated from a power-off condition and re-check its location and the database for available channels if it changes location during operation. A Mode II personal/portable device that has been in a powered state shall re-check its location and access the database daily to verify that the operating channel(s) continue to be available.

[2] 15.715 (f) Make its services available to all unlicensed TV band device users on a non-discriminatory basis.
[3] 15.715 (j) The database must have functionality such that upon request from the Commission it can indicate that no channels are available when queried by a specific TVBD or model of TVBDs.
[4] See Key Bridge Global LLC, *Proposal to Administer a TV Bands Database* submitted 01/04/09

Revise 15.713(e)(2) to read as follows:

> (2) Fixed and Mode II TVBDs shall not transmit unless they receive, from ~~the~~ an authenticated, FCC authorized TV bands database, a list of available channels.

Revise 15.715(f) to read as follows:

> (f) Make its services available to all valid unlicensed TV band device users on a non-discriminatory basis.

While we did not discuss it in the meeting, Key Bridge also wishes to note our support of and opposition to certain rule edits suggested by MSTV[5]. Specifically, we agree with the suggested paragraph §15.711 (b) (5), and the suggested text for §15.713 (a) (1). We do not support the suggested edits for §15.713 (e) (3) and (e) (4) and feel these would unnecessarily preclude allowed operating scenarios. We believe the suggested new text in paragraph §15.713 (e) (5) is confusing and could be simplified to explicitly require a status check of FCC device certification. We support the suggested edits for §15.715.

Best regards,

/s/

Jesse Caulfield, President

Key Bridge Global LLC

cc: Julius Knapp

Geraldine Matise

Walter Johnston

Ira Keltz

Hugh Van Tuyle

Peter Georgiu

Michael Ha

[5] See *Ex Parte* by MSTV and NAB dated 09/03/10, page 5-24.